UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/707,285	11/01/2000	Michael Brownlie	0500.0008210	8456

7590 05/07/2004

Christopher J. Reckamp
Vedder Price Kaufman & Kammholz
222 North LaSalle Street,
Suite 2600
Chicago,, IL 60601

EXAMINER	
WU, ALLEN S	

ART UNIT	PAPER NUMBER
2135	6

DATE MAILED: 05/07/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/707,285	Applicant(s) BROWNLIE ET AL.	
	Examiner Allen S. Wu	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 November 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 December 1997* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *6*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

1. Claim 12 is objected to because of the following informalities: improper grammar at last two lines of claim. Appropriate correction is required.

Double Patenting

2. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

3. Claims 1-8 and 10-38 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-35 of U.S. Patent No. 6,202,157 (hereinafter, Patent '157) in view of US Patent 5,167,988.

"A later patent claim is not patentably distinct from an earlier patent claim if the later claim is obvious over, or **anticipated by**, the earlier claim. In re Longi, 759 F.2d at 896, 225 USPQ at 651 (affirming a holding of obviousness-type double patenting because the claims at issue were obvious over claims in four prior art patents); In re Berg, 140 F.3d at 1437, 46 USPQ2d at 1233 (Fed. Cir. 1998) (affirming a holding of obviousness-type double patenting where a patent application claim to a genus is anticipated by a patent claim to a species within that genus). " ELI LILLY AND COMPANY v BARR

LABORATORIES, INC., United States Court of Appeals for the Federal Circuit, ON PETITION FOR REHEARING EN BANC (DECIDED: May 30, 2001).

As per claim 1 of the instant application, claim 1 of Patent '157, contains all the limitation of claim 1 of the instant application except obtaining the digital signature and the variable policy rule data from the means for storing, and not from a forwarded signed message. Matyas discloses using a master key which permits keys stored in a particular system's cryptographic key data set, the key encrypting key establishes a key-distribution channel which can be made unidirectional with at least one other network device or for each other device with which it wishes to communicate (see for example, col 4 ln 1 – col 5 ln 4). One of ordinary skill in the art at the time of the applicant's invention would have realized such a configuration that requires initial establishment and implementation of a network security policy by configuring stored data loaded into each device in the network. Furthermore, the means of specific data retrieval from a storage means that is not from a forwarded signed message is notoriously well known in the art. One of ordinary skill in the art at the time of the applicant's invention to recognize the providing means not from a forwarded signed message to provide the correct data to communicate with the device being inherently present within such a system. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Matyas within the claim limitations of the instant applications because it would have decreased overhead of processing data due to the absence of signed messages.

Claims 2-10 of Patent 6,202,157 contains all the elements of claims 2-8 and 10-11 of the instant application.

As per claim 12 of the instant application, claim 1 of Patent '157, contains all the limitation of claim 11 of the instant application except obtaining the digital signature and the variable policy rule data from the means for storing, and not from a forwarded signed message. Matyas discloses using a master key which permits keys stored in a particular system's cryptographic key data set, the key encrypting key establishes a key-distribution channel which can be made unidirectional with at least one other network device or for each other device with which it wishes to communicate (see for example, col 4 ln 1 – col 5 ln 4). One of ordinary skill in the art at the time of the applicant's invention would have realized such a configuration that requires initial establishment and implementation of a network security policy by configuring stored data loaded into each device in the network. Furthermore, the means of specific data retrieval from a storage means that is not from a forwarded signed message is notoriously well known in the art. One of ordinary skill in the art at the time of the applicant's invention to recognize the providing means not from a forwarded signed message to provide the correct data to communicate with the device being inherently present within such a system. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Matyas within the claim

limitations of the instant applications because it would have decreased overhead of processing data due to the absence of signed messages.

Claims 12-14 of Patent 6,202,157 contains all the elements of claims 13-15 of the instant application.

As per claim 16 of the instant application, claim 1 of Patent '157, contains all the limitation of claim 15 of the instant application except obtaining the digital signature and the variable policy rule data from the means for storing, and not from a forwarded signed message. Matyas discloses using a master key which permits keys stored in a particular system's cryptographic key data set, the key encrypting key establishes a key-distribution channel which can be made unidirectional with at least one other network device or for each other device with which it wishes to communicate (see for example, col 4 ln 1 – col 5 ln 4). One of ordinary skill in the art at the time of the applicant's invention would have realized such a configuration that requires initial establishment and implementation of a network security policy by configuring stored data loaded into each device in the network. Furthermore, the means of specific data retrieval from a storage means that is not from a forwarded signed message is notoriously well known in the art. One of ordinary skill in the art at the time of the applicant's invention to recognize the providing means not from a forwarded signed message to provide the correct data to communicate with the device being inherently present within such a

system. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Matyas within the claim limitations of the instant applications because it would have decreased overhead of processing data due to the absence of signed messages.

Claims 16-22 of Patent 6,202,157 contains all the elements of claims 17-21 and 23-24 of the instant application.

As per claim 22, the variable policy rule data including differing policy rule data for a plurality of software applications supported by at least one network node and wherein the at least one network node includes means for facilitating cryptographic processing of data that is accessible by the plurality of software applications is recited in claim 15 of Patent '157 (see col 10 ln 19-24).

As per claim 25 of the instant application, claim 23 of Patent '157, contains all the limitation of claim 11 of the instant application except obtaining the digital signature and the variable policy rule data from the means for storing, and not from a forwarded signed message. Matyas discloses using a master key which permits keys stored in a particular system's cryptographic key data set, the key encrypting key establishes a key-distribution channel which can be made unidirectional with at least one other network device or for each other device with which it wishes to communicate (see for example, col 4 ln 1 – col 5 ln 4). One of

ordinary skill in the art at the time of the applicant's invention would have realized such a configuration that requires initial establishment and implementation of a network security policy by configuring stored data loaded into each device in the network. Furthermore, the means of specific data retrieval from a storage means that is not from a forwarded signed message is notoriously well known in the art. One of ordinary skill in the art at the time of the applicant's invention to recognize the providing means not from a forwarded signed message to provide the correct data to communicate with the device being inherently present within such a system. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Matyas within the claim limitations of the instant applications because it would have decreased overhead of processing data due to the absence of signed messages.

Claims 24-26 of Patent 6,202,157 contains all the elements of claims 26-28 of the instant application.

As per claim 29 of the instant application, claim 27 of Patent '157, contains all the limitation of claim 11 of the instant application except obtaining the digital signature and the variable policy rule data from the means for storing, and not from a forwarded signed message. Matyas discloses using a master key which permits keys stored in a particular system's cryptographic key data set, the key encrypting key establishes a key-distribution channel which can be made

unidirectional with at least one other network device or for each other device with which it wishes to communicate (see for example, col 4 ln 1 – col 5 ln 4). One of ordinary skill in the art at the time of the applicant's invention would have realized such a configuration that requires initial establishment and implementation of a network security policy by configuring stored data loaded into each device in the network. Furthermore, the means of specific data retrieval from a storage means that is not from a forwarded signed message is notoriously well known in the art. One of ordinary skill in the art at the time of the applicant's invention to recognize the providing means not from a forwarded signed message to provide the correct data to communicate with the device being inherently present within such a system. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Matyas within the claim limitations of the instant applications because it would have decreased overhead of processing data due to the absence of signed messages.

Claims 28-30 of Patent 6,202,157 contains all the elements of claims 30 and 32-33 of the instant application.

As per claim 30 of the instant application, the variable policy rule data including differing policy rule data for a plurality of software applications supported by at least one network node and wherein the at least one network node includes means for facilitating cryptographic processing of data that is

accessible by the plurality of software applications is recited in claim 15 of Patent '157 (see col 10 ln 19-24).

As per claim 34 of the instant application, claim 31 of Patent '157, contains all the limitation of claim 11 of the instant application except obtaining the digital signature and the variable policy rule data from the means for storing, and not from a forwarded signed message. Matyas discloses using a master key which permits keys stored in a particular system's cryptographic key data set, the key encrypting key establishes a key-distribution channel which can be made unidirectional with at least one other network device or for each other device with which it wishes to communicate (see for example, col 4 ln 1 – col 5 ln 4). One of ordinary skill in the art at the time of the applicant's invention would have realized such a configuration that requires initial establishment and implementation of a network security policy by configuring stored data loaded into each device in the network. Furthermore, the means of specific data retrieval from a storage means that is not from a forwarded signed message is notoriously well known in the art. One of ordinary skill in the art at the time of the applicant's invention to recognize the providing means not from a forwarded signed message to provide the correct data to communicate with the device being inherently present within such a system. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Matyas within the claim

limitations of the instant applications because it would have decreased overhead of processing data due to the absence of signed messages.

Claims 32-35 of Patent 6,202,157 contains all the elements of claims 35-38 of the instant application.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas et al, US Patent 5,164,988, in view of Barlow, US Patent 5,204,961.

As per claims 1, 12, 16, 25, and 29, Matyas discloses a computer network security system having an enforceable security policy (see for example; abstract) comprising: means, operatively coupled to means for providing, for associating a digital signature of a central security policy rule data distribution source (see for example; certification center, col 11 ln 13-25) to the security policy rule data and means for storing the digital signature (see for example col 14 ln 54-col 15 ln 15); and network node means, operatively coupled to the storage means, for periodically obtaining the signature and the variable policy rule data from the means for storing (see for example, col 16 ln 10-25), and for

analyzing the variable policy rule data to facilitate unilateral security policy enforcement at a network node level (see for example; col 9 ln 15-51).

As for obtaining the signature and the variable policy rule data not from a forwarded signed message, Matyas further discloses using a master key which permits keys stored in a particular system's cryptographic key data set, the key encrypting key establishes a key-distribution channel which can be made unidirectional with at least one other network device or for each other device with which it wishes to communicate (see for example, col 4 ln 1 – col 5 ln 4). One of ordinary skill in the art at the time of the applicant's invention would have realized such a configuration that requires initial establishment and implementation of a network security policy by configuring stored data loaded into each device in the network. Furthermore, the means of specific data retrieval from a storage means that is not from a forwarded signed message is notoriously well known in the art. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to recognize the providing means not from a forwarded signed message to provide the correct data to communicate with the device being inherently present within such a system

Furthermore, Matyas does not explicitly teach a variable security policy. Barlow discloses a variable security policy rule data (see for example col 2 ln 18-21 and col 5 ln 20-29) including storing means for storing such a data (see for example, col 8 ln 63-col 9 ln 10). Both Matyas and Barlow disclose a means of providing a security policy over a network. Matyas further discloses providing

diverse levels of security among several client devices (see for example, col 8 ln 43-47). Being able to implement such levels in a flexible manner is important in the realm of security policies in networks where different policies need to be enforced according to the many variables at risk in a network. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Barlow within the system of Matyas because it would have increased the flexibility of for the central authority to implement and enforce different network policies for the different levels of a user, and also reduce such overhead by allowing for policy enforcement at the network nodes.

As per claims 2, 13, 17, 26, 35, Matyas-Barlow the disclose claim limitations above (see for example claim 1). Matyas further discloses means for providing a user interface means for facilitating selection of variable security policy rule data (see for example, col 12 ln 56-col 13 ln 14).

As per claims 3, 14, 27, Matyas-Barlow the disclose claim limitations above (see for example claim 1). Matyas further discloses means for providing the variable security policy rule data from a data file (see for example; fig 2 and col 13 ln 1-14).

As per claims 4, 15, 18, 28, and 36, Matyas-Barlow the disclose claim limitations above (see for example claim 1). Matyas further discloses selection of variable policy rule data on a per network node basis for central policy definition for the at least one network node (see for example, col 11 ln 5-13).

As per claims 5, 19, and 37, Matyas-Barlow the disclose claim limitations above (see for example claim 1). Matyas further discloses associating a digital signature to the variable policy rule data to create a policy certificate (see for example, col 11 ln 26-col 12 ln 9).

As per claims 6 and 20, Matyas-Barlow the disclose claim limitations above (see for example claim 1). Matyas further discloses means for storing policy rule data (see for example, col 5 ln 5-25); and means, operatively coupled to the means for storing, for using policy rule analysis data to decode the variable policy data to facilitate security policy enforcement at a network node level (see for example, col 11 ln 26-50).

As per claims 7, 32, and 38, Matyas-Barlow the disclose claim limitations above (see for example claim 1). Barlow further discloses variable policy rule data includes at least security policy identification data (security label) and policy rule setting data (see for example; col 3 ln 62-col 4 ln 29 and col 5 ln 20-30).

As per claims 8 and 21, Matyas-Barlow the disclose claim limitations above (see for example claim 1). Barlow further discloses variable policy rule data includes policy rule prioritization data (see for example, col 6 ln 44-53; trust realm is prioritized through which ream should be selected when more than one common realm exists).

As per claim 9, Matyas-Barlow the disclose claim limitations above (see for example claim 1). As for policy rule data includes policy rule data on a per application basis for a plurality of software applications supported by at least one network node, Matyas further discloses differing policy rules for several applications (clients) supported by the system (see for example, col 11 ln 1-13), therefore the policy rule data includes policy rule data on a per application basis for a plurality of applications (clients) supported by at least one network node. Barlow further discloses variable policy rule data on a per application basis (see for example col 3 ln 62-col 4 ln 12). The means of running software applications on each client is well known in the art. Furthermore, Barlow recognizes different software applications requiring different security policies (see for example, col 3 ln 62-66). One of ordinary skill in the art at the time of the applicant's invention would have recognized that the variable policy rule data includes policy rule data on a per application basis for the plurality of software applications on each of the clients.

As per claims 10 and 23, Matyas-Barlow the disclose claim limitations above (see for example claim 1). Matyas further discloses stores a policy certificate for distribution to the network node under control of the network node (see for example; col 6 ln 58-67).

As per claim 11, Matyas-Barlow the disclose claim limitations above (see for example claim 1). Matyas further discloses stores a policy certificate for distribution to the network nodes under control of the means for associating (see for example; col 9 ln 15-51).

As per claims 22 and 31, Matyas-Barlow the disclose claim limitations above (see for example claim 16). Matyas further discloses policy rule data includes differing policy rule data for a plurality of software applications supported by at least one network node (see for example; col 11 ln 1-13). The means of running software applications on each client is well known in the art. Furthermore, Barlow recognizes different software applications requiring different security policies (see for example, col 3 ln 62-66). One of ordinary skill in the art at the time of the applicant's invention would have recognized that the variable policy rule data includes policy rule data on a per application basis for the plurality of software applications on each of the clients.

Matyas further discloses wherein the at least one network node includes means for facilitating cryptographic processing of data that is accessible by the plurality of software applications (see for example; col 10 ln 41-61).

As per claim 11, Matyas-Barlow the disclose claim limitations above (see for example claim 1). Matyas further discloses stores a policy certificate for distribution to the network nodes under control of a network server (see for example; fig 1 and col 10 ln 41-61). Network servers are well known in the art to provide services such as distribution of data to network nodes. One of ordinary skill in the art at the time of the applicant's invention would have recognized the certification authority to be such a network server for controlling distribution of policy certificates in such a system.

As per claim 30, Matyas-Barlow the disclose claim limitations above (see for example claim 29). Matyas further discloses means for storing variable policy rule data (see for example, col 5 ln 5-25), and wherein the means for analyzing the variable policy rule data includes means for storing policy rule analysis data for evaluating the policy rule data (see for example; col 11 ln 42-50) and means, operatively coupled to the means for storing and the means for storing policy rule analysis data, for using the policy rule analysis data to decode the variable policy rule data to facilitate security policy enforcement at a network level (see for example, col 11 ln 26-50).

As per claim 33, Matyas-Barlow the disclose claim limitations above (see for example claim 29). Matyas further discloses the variable policy rule data includes policy rule prioritization data (see for example, col 6 ln 44-53; trust realm is prioritized through which ream should be selected when more than one common realm exists) and wherein the means for periodically obtaining obtains a digital signature corresponding to the policy rule data (see for example, col 11 ln 26-col 12 ln 9).

As per claim 34, Matyas discloses means for storing programming instructions (see for example col 12 ln 10-20) that facilitate storing variable security policy rule data for use by a network node (see for example col 14 ln 54-col 15 ln 15); and means for storing programming instructions (see for example col 12 ln 10-20) that facilitate providing the variable security policy rule data for distributions to at least one network node (see for example, col 16 ln 10-25) to facilitate unilateral security policy enforcement at a network level (see for example; col 9 ln 15-51).

As for obtaining variable policy rule data not from a forwarded signed message, Matyas further discloses using a master key which permits keys stored in a particular system's cryptographic key data set, the key encrypting key establishes a key-distribution channel which can be made unidirectional with at least one other network device or for each other device with which it wishes to

communicate (see for example, col 4 ln 1 – col 5 ln 4). One of ordinary skill in the art at the time of the applicant's invention would have realized such a configuration that requires initial establishment and implementation of a network security policy by configuring stored data loaded into each device in the network. Furthermore, the means of specific data retrieval from a storage means that is not from a forwarded signed message is notoriously well known in the art. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to recognize the providing means not from a forwarded signed message to provide the correct data to communicate with the device being inherently present within such a system

Furthermore, Matyas does not explicitly teach a variable security policy. Barlow discloses a variable security policy rule data (see for example col 2 ln 18-21 and col 5 ln 20-29) including storing means for storing such a data (see for example, col 8 ln 63-col 9 ln 10). Both Matyas and Barlow disclose a means of providing a security policy over a network. Matyas further discloses providing diverse levels of security among several client devices (see for example, col 8 ln 43-47). Being able to implement such levels in a flexible manner is important in the realm of security policies in networks where different policies need to be enforced according to the many variables at risk in a network. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Barlow within the system of Matyas because it would have increased the flexibility of for the central authority to

implement and enforce different network policies for the different levels of a user, and also reduce such overhead by allowing for policy enforcement at the network nodes.

As per claim 39, Matyas-Barlow the disclose claim limitations above (see for example claim 1). Matyas further discloses central security policy rule data distribution source is a certification authority (see for example; certification authority, col 10 ln 62-65).

As per claim 40, Matyas-Barlow the disclose claim limitations above (see for example claim 1). Barlow further discloses variable policy rule data includes policy rule data on a per node basis (see for example; col 3 ln 62-66).

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US Patent 5,828,832, to Holden et al, discloses a means of enforcing a multi-level security policy in a computer network.

US Patent 5,903,652, to Mital, discloses a means of enforcing and distribution of a security policy.

US Patent 6,119,230, to Carter discloses variable security policies in a distributed computer system.

US Patent 6,158,007, to Moreh et al discloses a security system for different software applications.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Allen S. Wu whose telephone number is 703-305-0708. The examiner can normally be reached on Monday-Friday 9am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Allen Wu
Patent Examiner
Art Unit 2135

ASW